
Critical Foundations

Protecting America's Infrastructures

The Report of the President's Commission
on Critical Infrastructure Protection

October 1997

(Intentionally Left Blank)



PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION

October 13, 1997

The President
The White House
Washington, DC 20500

Dear Mr. President:

It is a privilege to forward the report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations*. You asked us to study the critical infrastructures that constitute the life support systems of our nation, determine their vulnerabilities and propose a strategy for protecting them into the future. I believe our report does this.

There is no doubt that our critical infrastructures are the best in the world—largely the result of the tremendous efficiency and global reach made possible by incorporation of our rapidly advancing information and communication technology. In fact, we found all our infrastructures increasingly dependent on information and communications systems that criss-cross the nation and span the globe. That dependence is the source of rising vulnerabilities and, therefore, it is where we concentrated our effort.

We found no evidence of an impending cyber attack which could have a debilitating effect on the nation's critical infrastructures. While we see no electronic disaster around the corner, this is no basis for complacency. We did find widespread capability to exploit infrastructure vulnerabilities. The capability to do harm—particularly through information networks—is real; it is growing at an alarming rate; and we have little defense against it.

Because the infrastructures are mainly privately owned and operated, we concluded that critical infrastructure assurance is a shared responsibility of the public and private sectors. The only sure path to protected infrastructures in the years ahead is through a real partnership between infrastructure owners and operators and the government. Consequently, in addition to our recommendations about improving our government's focus on infrastructure assurance in the Information Age, you will find some recommendations for collaborative public and private organizational arrangements that challenge our conventional way of thinking about government and private sector interaction.

Thank you for the opportunity to serve our nation on this Commission, and for the chance to work with a talented and patriotic group of Commissioners and staff from both government and the private sector.

Respectfully,

A handwritten signature in dark ink, reading "Robert T. Marsh". The signature is fluid and cursive, with the first name "Robert" being more prominent.

Robert T. Marsh
Chairman

(Intentionally Left Blank)

President's Commission on Critical Infrastructure Protection

COMMISSIONERS

Robert T. Marsh, *Chairman*

John R. Powers, *Executive Director — Federal Emergency Management Agency*

Merritt E. Adams — *AT&T*

Richard P. Case — *IBM*

Mary J. Culnan — *Georgetown University*

Peter H. Daly — *Department of the Treasury*

John C. Davis — *National Security Agency*

Thomas J. Falvey — *Department of Transportation*

Brenton C. Greene — *Department of Defense*

William J. Harris — *Association of American Railroads*

David A. Jones — *Department of Energy*

William B. Joyce — *Central Intelligence Agency*

David V. Keyes — *Federal Bureau of Investigation*

Stevan D. Mitchell — *Department of Justice*

Joseph J. Moorcones — *National Security Agency*

Irwin M. Pikus — *Department of Commerce*

William Paul Rodgers, Jr. — *National Association of Regulatory Utility Commissioners*

Susan V. Simens — *Federal Bureau of Investigation*

Frederick M. Struble — *Federal Reserve Board*

Nancy J. Wong — *Pacific Gas and Electric Company*

EXECUTIVE STAFF

Phillip E. Lacombe, *Staff Director*

James H. Kurtz, COL, USA, *Chief of Staff/Executive Secretary*

Janet B. Abrams, *Director of External Affairs/White House Liaison*

Robert E. Giovagnoni, Col, USAF, *General Counsel*

Adrienne M. Griffen, *Executive Assistant to the Chairman*

Elizabeth (Betsy) Harrison, *Director of Legislative Affairs*

Brian P. Hoey, Lt Col, USAF, *Executive Assistant to the Chairman*

Nelson M. McCouch III, MAJ, USA, *Director of Public Affairs*

Monica Y. McNeil, *Executive Assistant to the Chief of Staff/Assistant Executive Secretary*

Annie N. Nelson, *Director of Administration*

Carla L. Sims, *Director of Public Affairs*

Lawrence P. St. Marie, SMSgt, USAF, *Executive Officer*

Sona A. Viridi, *Executive Assistant to the Staff Director*

PROFESSIONAL STAFF

Elizabeth A. Banker
Gary R. Boyd
Patricia E. Burt
Julie Consilvio
Frederick S. Davidson
L. C. J. Jacobson
Gary P. Kosciusko

Lloyd E. Lutz Jr., Lt Col, USAF
Carol M. Medill
T. Lynette Proctor
Pamela D. Saunders
James J. Stekert
Stephen T. York

SUPPORT STAFF

Bernard R. Robinson, *Deputy Director of Administration*
Bonnie L. Julia, SFC, USA, *NCOIC*

Karen R. Allen, SrA, USAF
Robert W. Boyd, YN2, USN
Joseph A. Broadway, YN1, USN
Patrick Barlow
Eric J. Cline
James E. Crawford, SSG, USA
Debra A. Dawson, SSG, USA
Roda Dickerson, SrA, USAF
Elizabeth S. Ellingboe, SSgt, USAF
Jeffrey G. Estep, SSgt, USAF
Troy L. Joyner, SSG, USA
Peter D. LeNard

Becky Love
Gerald T. Posey, TSgt, USAF
Sandra M. Robinson, SSgt, USAF
Sandra L. Scroggs
Mike Seabron
Sherrie M. Smith, SGT, USA
Sharon S. Strippoli
Shawn R.L. Vincent, Sgt, USAF
Scott A. Ward
Brian W. Young, SrA, USAF
Ed Young

SENIOR CONSULTANTS

William A. Buehring
Mary F. Dunham
Ron E. Fisher
Paul W. Hanley
Peter Gossens
Duane G. Harder
Michael T. Hovey
Joelle Jordan

Ramesh Maraj
Gabe Maznick
Willis J. Ozier
Paul Byron Pattak
James P. Peerenboom
George J. Rothstein
Lee M. Zeichner

And special thanks to the following for their advice and support:

Ed Appel
Frederick L. Frostic
Bill Garber
Seymour Goodman
David Graham
Michael Leonard
Stephen J. Lukasik

Paul H. Richanbach
Kathleen Robertson
Elizabeth Sauer
Paula Scalingi
James Schlesinger
Suzy Tichenor
Larry Welch

C o n t e n t s

	Page
Foreword	vii
Executive Summary	ix
Part One: The Case for Action	1
Chapter One Acting Now to Protect the Future	3
Chapter Two The New Geography	7
Chapter Three New Vulnerabilities, Shared Threats, Shared Responsibility	11
Chapter Four Findings and Policy	21
Part Two: A Strategy for Action	25
Chapter Five Establishing the Partnership	27
Chapter Six Building the Partnership	35
Chapter Seven Structuring the Partnership	47
Chapter Eight Report on Awareness and Education	67
Chapter Nine Leading by Example	73
Chapter Ten Legal Initiatives	79
Chapter Eleven Research and Development	89
Chapter Twelve Implementation Strategy	93
Onward	101
Appendices	
Appendix A Sector Summary Reports	A-1
Appendix B Glossary	B-1

(Intentionally Left Blank)

F o r e w o r d

The task given us by the President was daunting. America's critical infrastructures underpin every aspect of our lives. They are the foundations of our prosperity, enablers of our defense, and the vanguard of our future. They empower every element of our society. There is no more urgent priority than assuring the security, continuity, and availability of our critical infrastructures.

After fifteen months of evaluating the infrastructures, assessing their vulnerabilities, and deliberating assurance alternatives, our fundamental conclusion is that we have to think differently about infrastructure protection today and for the future.

We found that the nation is so dependent on our infrastructures that we must view them through a national security lens. They are essential to the nation's security, economic health, and social well being. In short, they are the lifelines on which we as a nation depend.

We also found the collective dependence on the information and communications infrastructure drives us to seek new understanding about the Information Age. Essentially, we recognize a very real and growing cyber dimension associated with infrastructure assurance.

In the cyber dimension there are no boundaries. Our infrastructures are exposed to new vulnerabilities—cyber vulnerabilities—and new threats—cyber threats. And perhaps most difficult of all, the defenses that served us so well in the past offer little protection from the cyber threat. Our infrastructures can now be struck directly by a variety of malicious tools.

Our new thinking must accommodate the cyber dimension. We must develop a new set of “street smarts” to deal with it, and we must apply them in new ways. One of the most important is recognizing that the owners and operators of our critical infrastructures are now on the front lines of our security effort. They are the ones most vulnerable to cyber attacks. And that vulnerability jeopardizes our national security, global economic competitiveness, and domestic well being.

It is with this in mind that we offer our report.

(Intentionally Left Blank)

Executive Summary

Critical Foundations Protecting America's Infrastructures

“Our responsibility is to build the world of tomorrow by embarking on a period of construction—one based on current realities but enduring American values and interests”

— President William J. Clinton, “A National Security Strategy for a New Century,” May 1997

Introduction

Our national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society. These critical infrastructures—energy, banking and finance, transportation, vital human services, and telecommunications—must be viewed in a new context in the Information Age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence. This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk.

For most of our history, broad oceans, peaceable neighbors and our military power provided all the infrastructure protection we needed. But just as the terrible long-range weapons of the Nuclear Age made us think differently about security in the last half of the 20th Century, the electronic technology of the Information Age challenges us to invent new ways of protecting ourselves now. We must learn to negotiate a new geography, where borders are irrelevant and distances meaningless, where an enemy may be able to harm the vital systems we depend on without confronting our military power. National defense is no longer the exclusive preserve of government, and economic security is no longer just about business. The critical infrastructures are central to our national defense and our economic power, and we must lay the foundations for their future security on a new form of cooperation between government and the private sector.

The Case for Action

A satchel of dynamite and a truckload of fertilizer and diesel fuel are known terrorist tools. Today, the right command sent over a network to a power generating station's control computer could be just as devastating as a backpack full of explosives, and the perpetrator would be more difficult to identify and apprehend.

The rapid growth of a computer-literate population ensures that increasing millions of people around the world possess the skills necessary to conduct such an attack. The wide adoption of common protocols for system interconnection and the availability of "hacker tool" libraries make their task easier.

While the possibility of chemical, biological, and even nuclear weapons falling into the hands of terrorists adds a new and frightening dimension to physical attacks, such weapons are difficult to acquire. In contrast, the resources necessary to conduct a cyber attack have shifted in the past few years from the arcane to the commonplace. A personal computer and a telephone connection to an Internet Service Provider anywhere in the world are enough to cause harm.

Growing complexity and interdependence, especially in the energy and communications infrastructures, create an increased possibility that a rather minor and routine disturbance can cascade into a regional outage. Technical complexity may also permit interdependencies and vulnerabilities to go unrecognized until a major failure occurs.

We know our infrastructures have substantial vulnerabilities to domestic and international threats. Some have been exploited—so far chiefly by insiders. Although we know these new vulnerabilities place our infrastructures at risk, we also recognize that this is a new kind of risk that requires new thinking to develop effective countermeasures. Coping with increasingly cyber-based threats demands a new approach to the relationship between government and the private sector. Because it may be impossible to determine the nature of a threat until after it has materialized, infrastructure owners and operators—most of whom are in the private sector—must focus on protecting themselves against the tools of disruption, while the government helps by collecting and disseminating the latest information about those tools and their employment. This cooperation implies a more intimate level of mutual communication, accommodation, and support than has characterized public-private sector relations in the past.

The Commission has not discovered an immediate threat sufficient to warrant a fear of imminent national crisis. However, we are convinced that our vulnerabilities are increasing steadily, that the means to exploit those weaknesses are readily available and that the costs associated with an effective attack continue to drop. What is more, the investments required to improve the situation—now still relatively modest—will rise if we procrastinate.

We should attend to our critical foundations before we are confronted with a crisis, not after. Waiting for disaster would prove as expensive as it would be irresponsible.

A Strategy for Action

The Commission recommends several practical measures to realize our vision of a new government-private sector partnership.

The quickest and most effective way to achieve a much higher level of protection from cyber threats is a strategy of cooperation and information sharing based on partnerships among the infrastructure owners and operators and appropriate government agencies.

To facilitate this new relationship between government and industry, new mechanisms will be needed, including sector “clearing houses” to provide the focus for industry cooperation and information sharing; a council of industry CEOs, representatives of state and local government, and Cabinet secretaries to provide policy advice and implementation commitment; a real-time capability for attack warning; and a top-level policy making office in the White House.

Other measures are also required. Infrastructure protection must be ingrained in our culture, beginning with a comprehensive program of education and awareness. This includes both infrastructure stakeholders and the general public, and must extend through all levels of education, both academic and professional.

The federal government must lead the way into the Information Age by example, tightening measures to protect the infrastructures it operates against physical and cyber attack.

The government can also help by streamlining and clarifying elements of the legal structure that have not kept pace with technology. Some laws capable of promoting assurance are not as clear or effective as they could be. Others can operate in ways that may be unfriendly to security concerns. Sorting them out will be an extensive undertaking, involving efforts at local, state, federal, and international levels. We have offered a number of preliminary legal recommendations intended to jump-start this process of reform.

Another area where government must lead is in research and development. Some of the basic technology and tools needed to provide improved infrastructure protection already exist, but need to be widely employed. However, there is a need for additional technology with which to protect our essential systems. We have, therefore, recommended a program of research and development focused on those needed capabilities.

In summary, all of us need to recognize that the cyber revolution brings us into a new age as surely as the industrial revolution did two centuries ago. Now, as then, our continued security requires a reordering of national priorities and new understanding about our respective roles in support of the national goals. The relationships that have stood us in such good stead through the end of the second millennium must give way to new ones better suited to the third.

(Intentionally Left Blank)